RSAC 2025 Conference

Many Voices.
One Community.

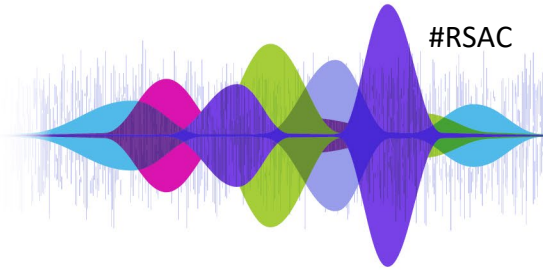
SESSION ID: NCS-T02

The Inevitable Collision Between 5G and Zero Trust: Real Life Solutions

Anubhav Arora
VP, Security Engineering
Ericsson Enterprise Wireless

Chase Cunningham
Dr. Zero Trust
Lumu Technologies

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

The New World

5G Impact on Security

- Scale of mobility
- Devices + Users
- 5G Public/Private
- 5G Security

Zero Trust Journey

- Implementation
- Policy Journey
- Operations

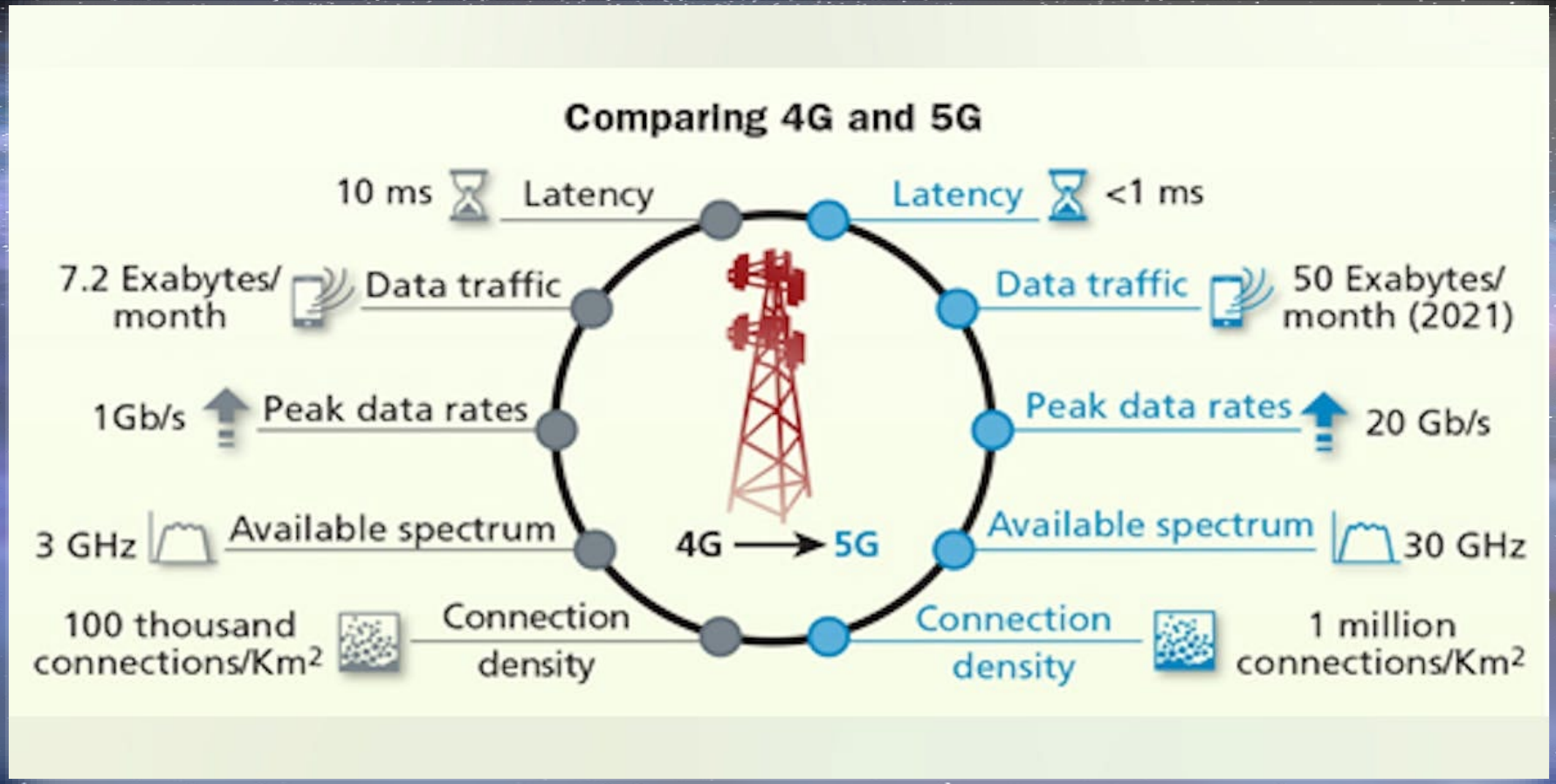
Common Use Cases

- First Responders
- Smart Cities / IoT
- Energy and OT

Apply Takeaways

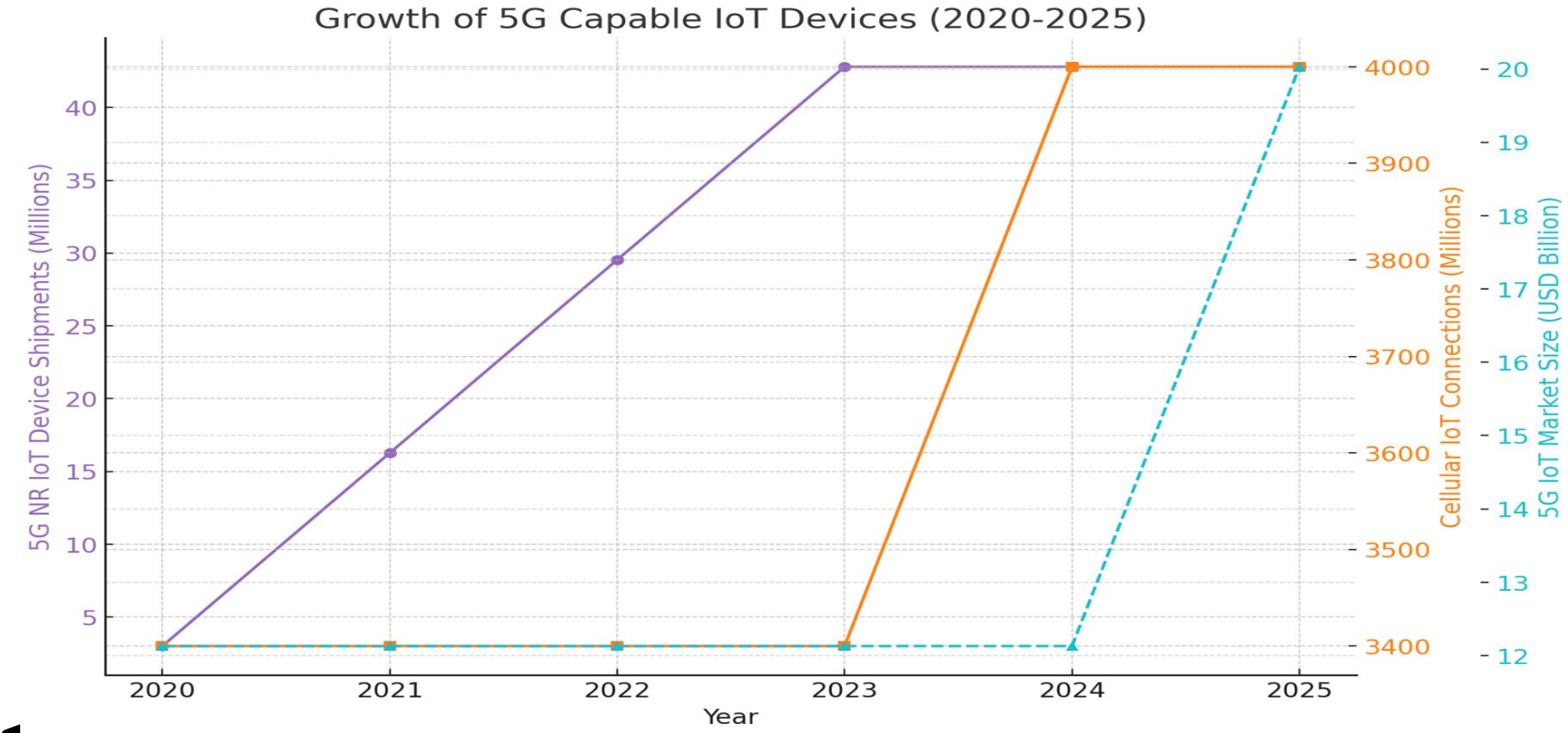
Everything is "connected" now

No more networks, it's universes...



5G Mobility → Enterprise Transformation

Devices Grow On



ZT and 5G...

PERMITER SECURITY
SECURITY
ZERO TRUST
SECURITY
ZERO
SECURITY
ZERO TRUST
SECURITY
ZERO TRUST
SECURITY
ZERO TRUST
SECURITY

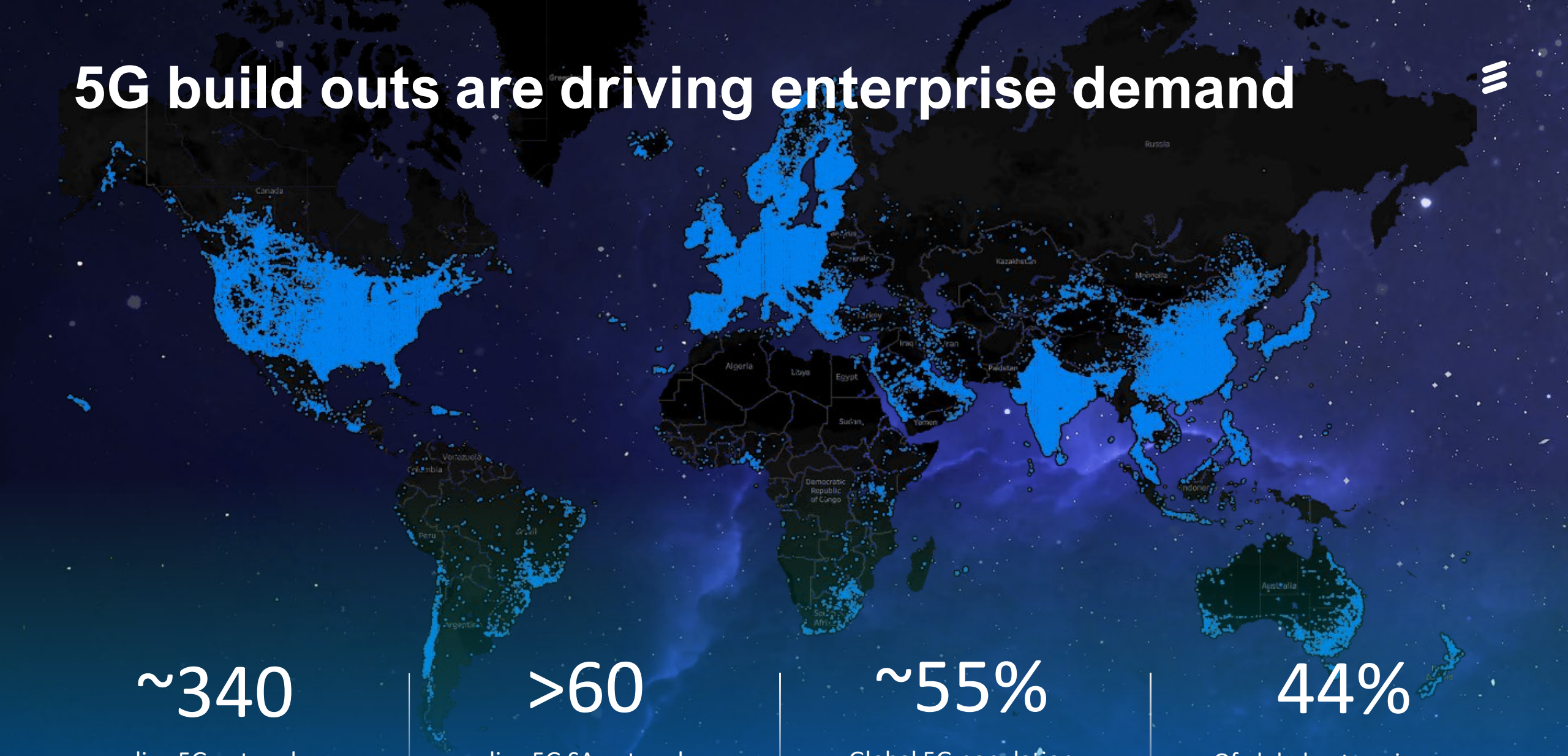
Saving where it matters...

RSAC 2025 Conference

5G Impact on Security

Many Voices.
One Community.

5G build outs are driving enterprise demand



~340

live 5G networks
(GSA, Dec 2024, all vendors)

>60

live 5G SA networks
(GSA, Dec 2024 all vendors)

~55%

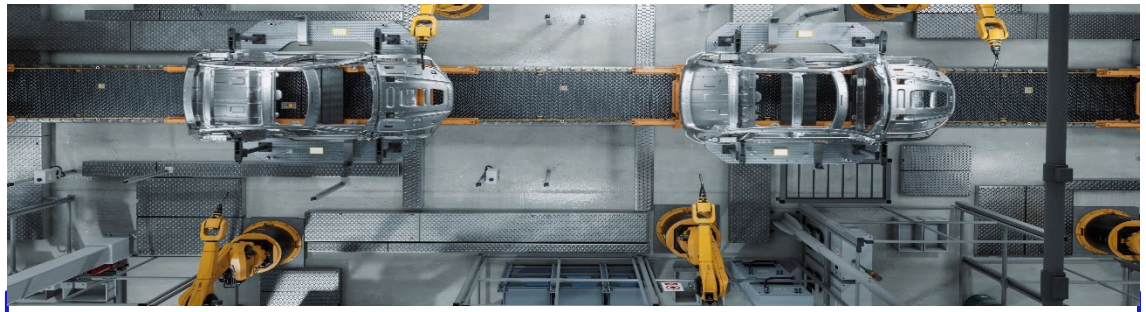
Global 5G population coverage by end of 2024

44%

Of global enterprises are increasing their investments in 5G (IDC, 2024)

Source: Ericsson Mobility Report, Nov 2024

Options for 5G in the enterprise



Private 5G Networks

DEDICATED NETWORK

Private 5G solutions use dedicated infrastructure on licensed spectrum

- ✓Critical industrial environments
- ✓Better coverage and mobility support
- ✓Network visibility and control
- ✓3GPP standards compliance

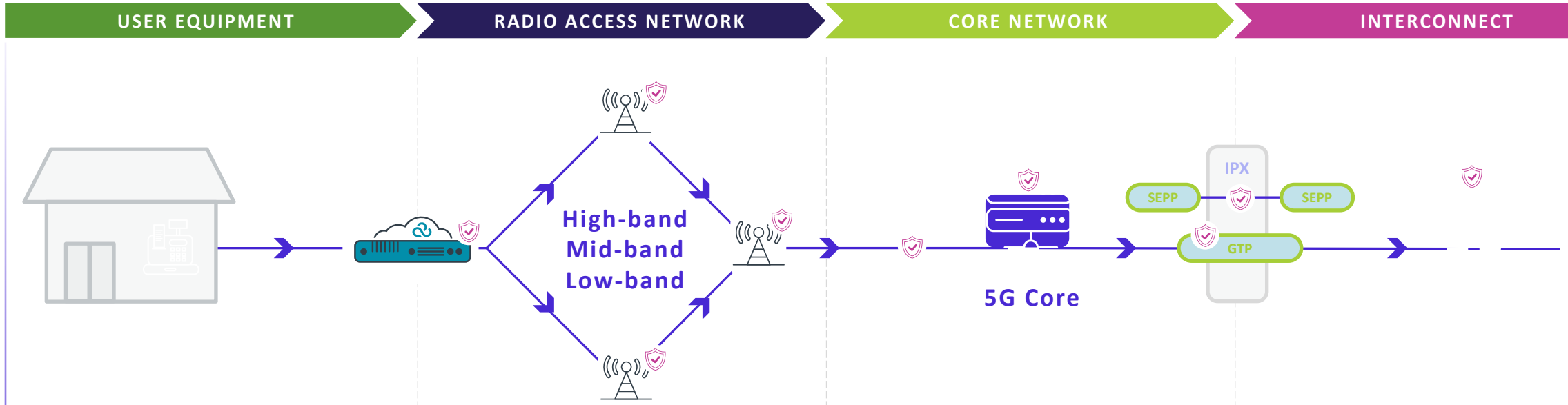
Public 5G Networks

WIRELESS WAN WITH TELCO NETWORKS

Leverages the carrier macro network to provide connectivity for vehicles, IoT devices, and sites

- ✓Requires security just like other WAN technologies
- ✓Carrier delivered private APNs is an option
- ✓Zero-trust can play a key role in securing WWANs

5G Supports Zero-Trust Principles



UE THREATS: **Enhanced Auth framework**

Standardized on Extensible Authentication Protocol (EAP)

PRIVACY THREATS: **Enhanced subscriber privacy**

IMSI equivalent is transmitted in encrypted channel

RAN AND ROGUE BASE STATION THREATS: **Advanced integrity protection of UPF**

User plane traffic has stronger encryption (256-bit)
Slices enable security policy separation and DDoS mitigation

CORE NETWORK THREATS: **Improved core network agility and security**

Network functions are service based, authenticated and encrypted using mTLS

ROAMING THREATS:

Expanded roaming security

SEPP: Encryption of all traffic including from operator to operator

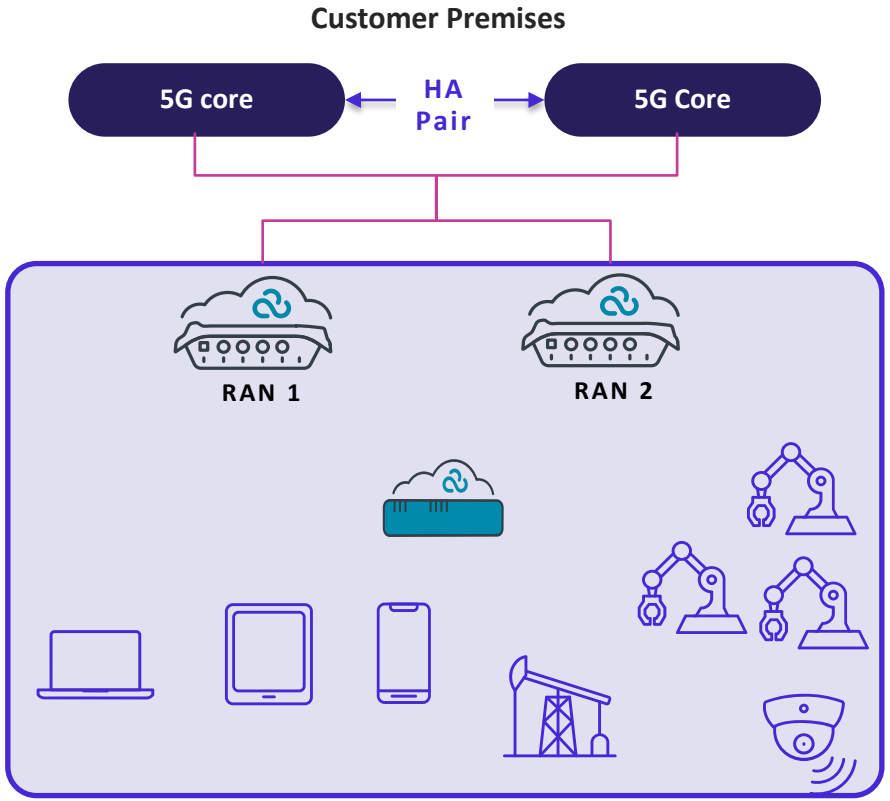
Private 5G: Supports ZT Principles

5G Core and RAN

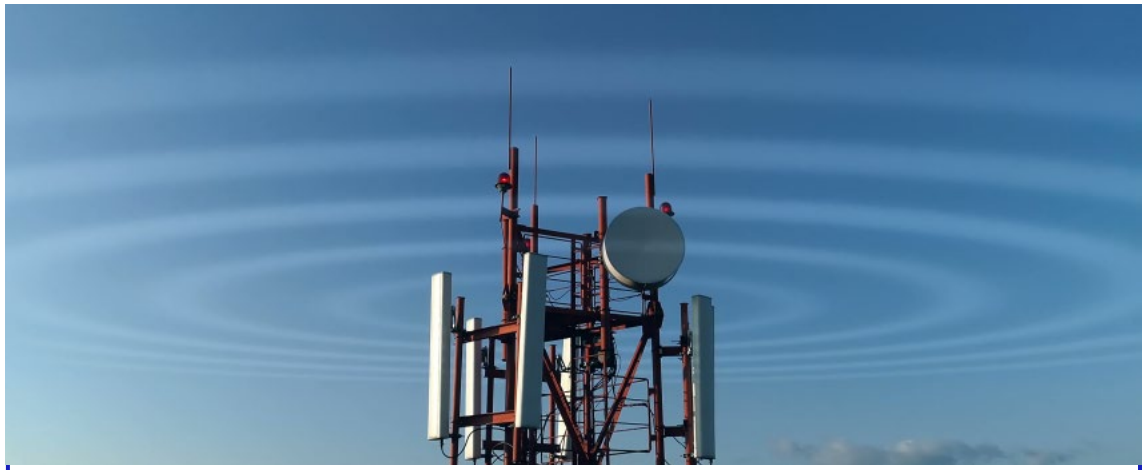
- Service based architecture
- Encryption and mTLS
- Policy based access controls

UE Behavior

- SIM and/or UE device-based authentication
- SIM <> UE Device enforcement
- UE Device type fingerprinting
- UE Device activity monitoring

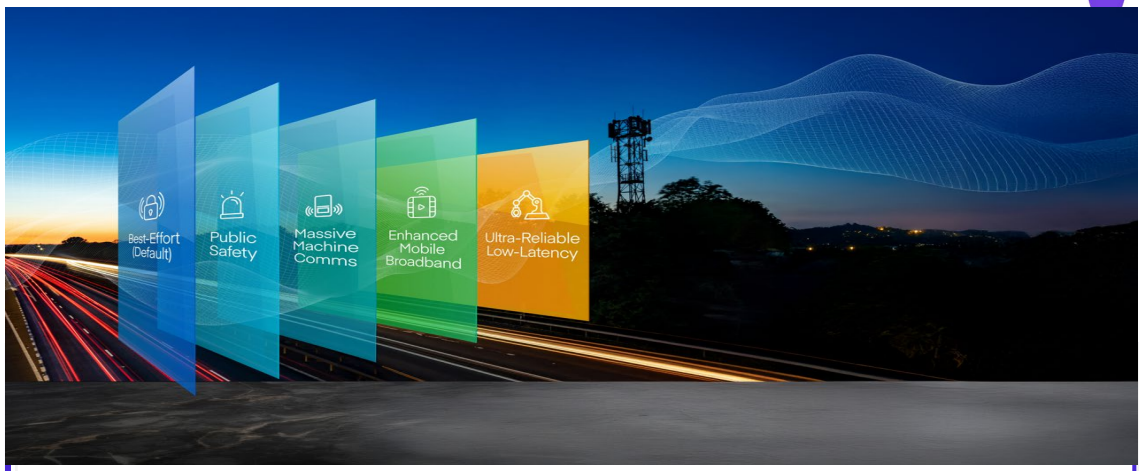


5G: A New Secure Network Edge



5G (SA/Advanced) is secure

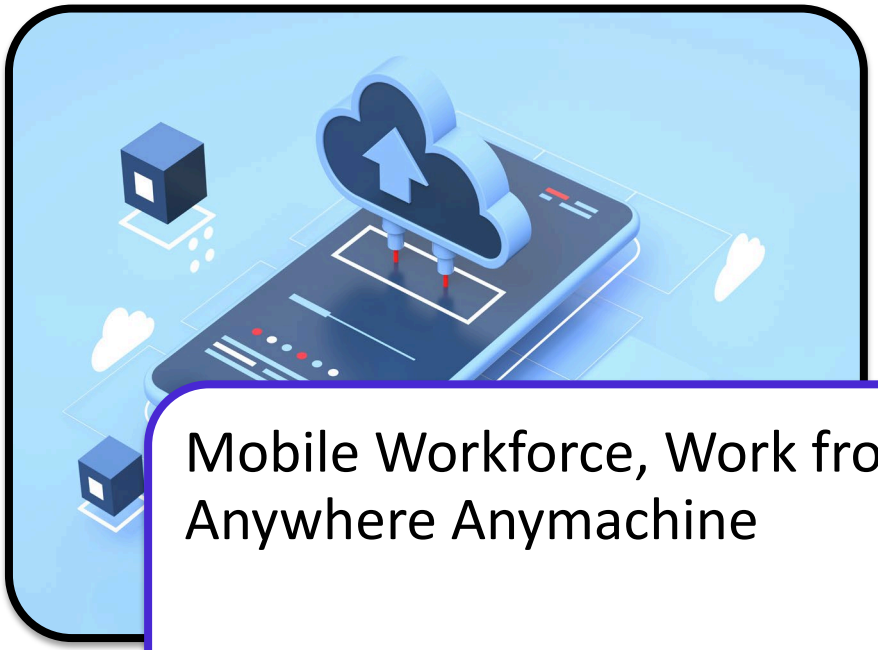
- Networks are inherently secure (Radio / Infra)
- Products can integrate 5G Authenticated Identity in policy primitives



5G is a new wide edge

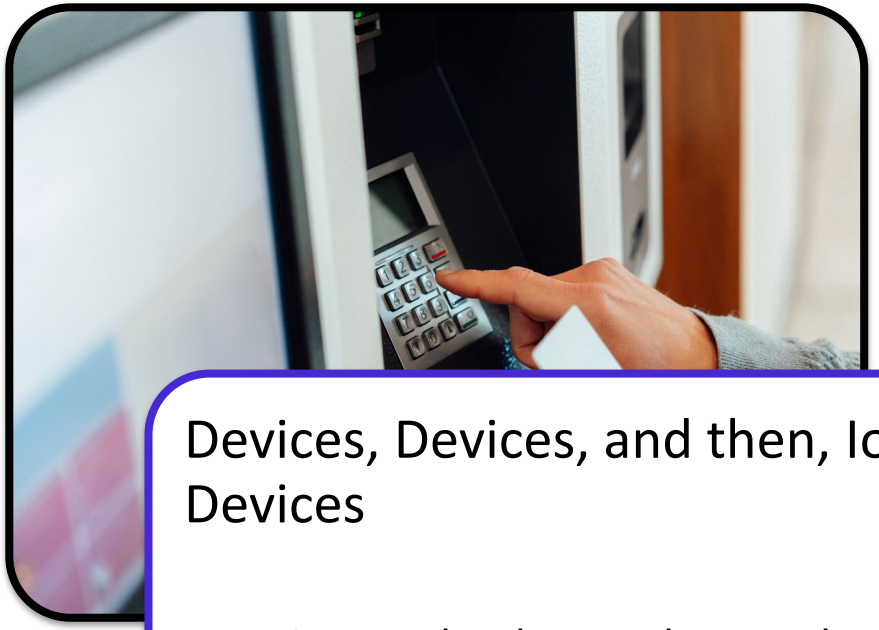
- Identity authenticated by SIM
- Location is available from network
- WAN segmentation uses 5G Slices

Impact: Proliferation of the Untrusted



Mobile Workforce, Work from Anywhere Anymachine

- Employees use mobile devices with fewer security controls
- Employee and contractor access via unmanaged BYOD is a security challenge



Devices, Devices, and then, IoT Devices

- Devices are hard to patch, many have backend servers in other countries
- Segmented networks for devices are difficult for usability reasons
- Devices are sometimes hard to isolate, and provide an ‘Initial Access’

Zero Trust: The Right Security Posture

External darknet

Internal micro-segmentation

Invisible private resources

Secure then Connect

Least Privilege Access Policy

Internet: Prevent, Isolate, then Detect

Continuous Monitoring, Analytics

Alerts Triage Hunting

RSAC™ 2025 Conference

Implementation Journey

Many Voices.
One Community.

Choose the right Cellular + Security Solution

5G WAN FUNCTIONS DIFFERENTLY THAN WIRED WAN

Mobile locations

No concept of fixed bandwidth

Predominately metered connections

CHOOSE A SOLUTION DESIGNED FOR THE UNIQUENESS OF 5G

RESILIENCY

Traffic steering based on cellular attributes

Use of in-line traffic for WAN measurements

5G networks evolving to 5G Stand-Alone

SECURITY

Leverage Slices for Segmentation

SIM authentication

Common policy between public & private 5G

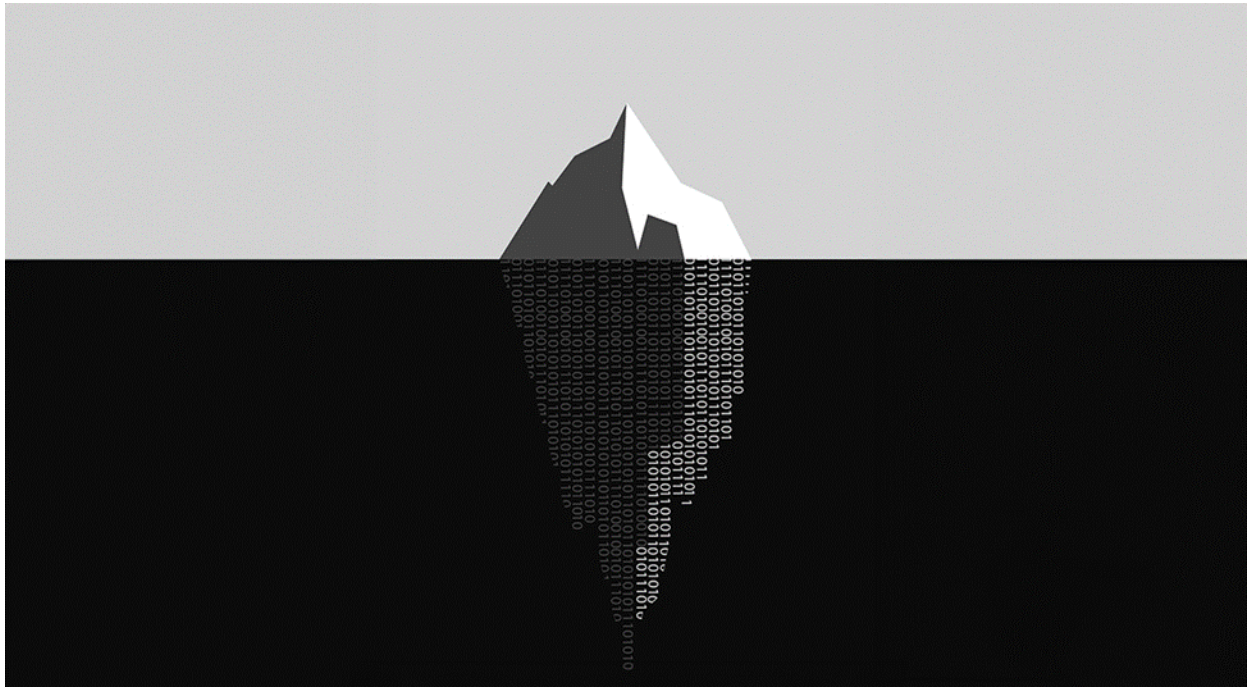
Zero-Trust Network Architecture

Darknet

Reduced external attack surface

- Inside-out edge to cloud, encrypted
- Secured by 5G from MITM
- No scanning / recon possible
- No leakage of internal IP space
- Internally resolved FQDNs

Network, applications: Invisible

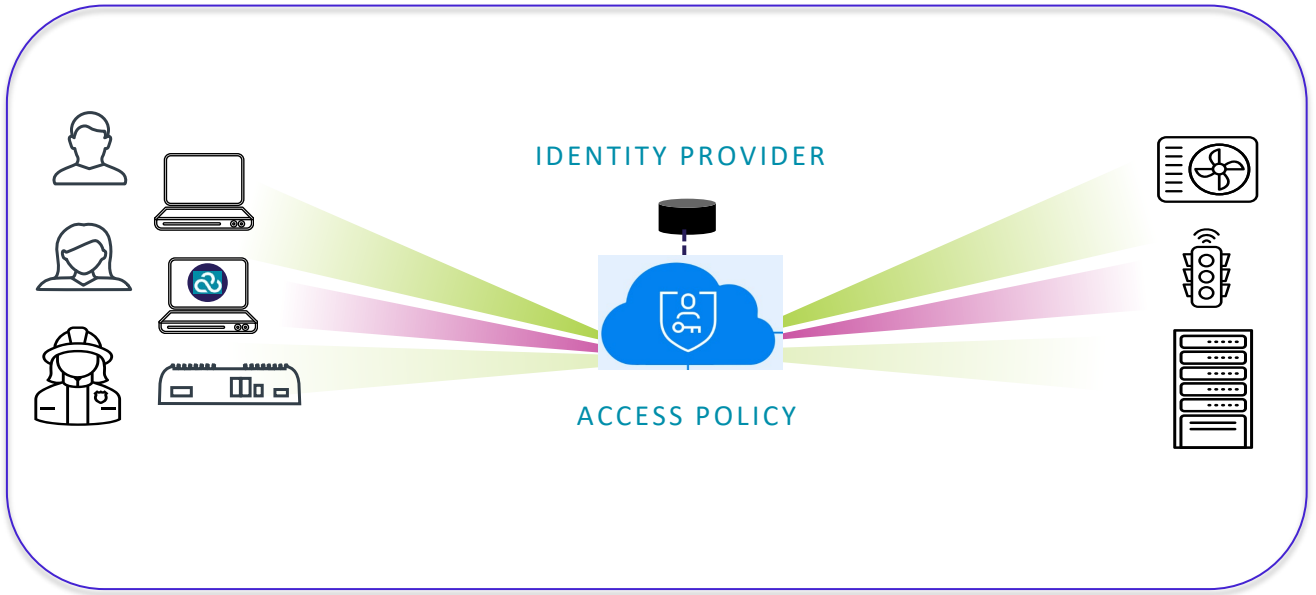


Zero-Trust Network Architecture

Segmented

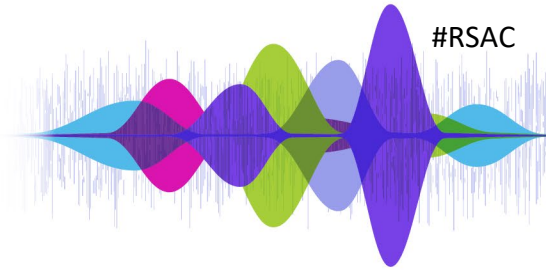
No lateral movement

- No network access or scanning possible
- Access to applications if and only if flow allowed by policy
- Segmentation using 5G slices for separate LANs or networks
- Use Private 5G as needed



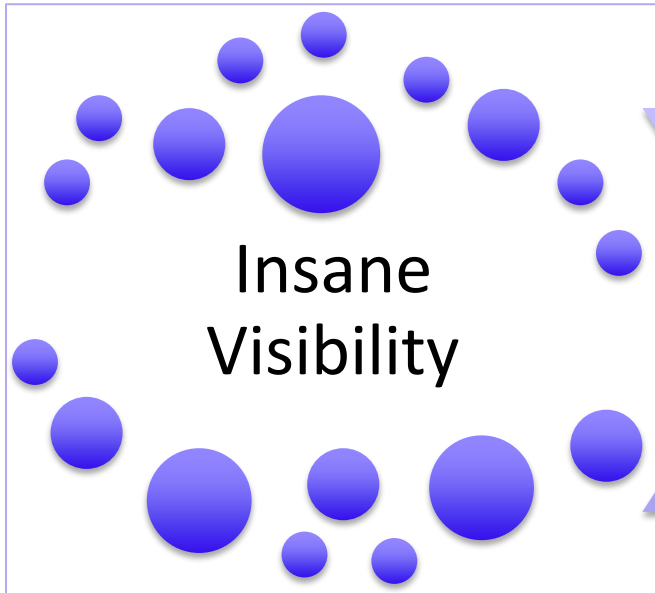
Least privilege and always verified: Limited blast radius

Zero Trust Policy Architecture



Internal Access: "Default Invisible"	Internet Traffic: "Prevent then Detect"	Unmanaged Devices: "Isolated Access"
No implicit trust, always verified	**Prevent then detect leads to actionable alerts**	**Protection from ALL untrusted assets**
• Identity of user or device, use 5G identifiers • Use context & attributes, like device posture, location and attributes from 5G • Restrict users, devices to access specific needed applications only	• Implement strict internet bound controls with IPS, NGFW, SWG, DLP, CASB • For any medium or high-risk traffic, use isolated access with RBI or Secure Access portal that uses isolation	• Untrusted devices are a potential compromise • Access only through isolated portal • Incorporate identity and application-based policy for non-employees

Zero Trust Operational Process



Continuous Monitoring

Actionable Alerts

Get visibility into ALL traffic

NTA/NDR traffic analytics

Anomaly detection

Monitor, analyze anomalies

Continuously improve policy

Use device posture in policy

All violations actionable

Utilize isolation to limit risk

Implement alert triage

Use threat hunting as needed

RSAC 2025 Conference

Common Use Cases

First Responders: Mission Critical

CRITICAL NEEDS

- Dedicated cellular connectivity in emergencies
- Highly reliable mobile internet access
- Resilient & secure mission critical application access
- Policy for identity regardless of WAN or location
- Segmentation of mission critical vs other traffic

VALIDATED ARCHITECTURE THAT PROVIDES

- Priority access, evolving to dedicated with slicing - prioritized public safety slices
- High availability with WAN bonding
- ZTNA for secure remote access to private apps
- Single policy that follows identity
- Micro-Segmentation of local LANs

Smart Cities: Networks of IoT

CRITICAL NEEDS

- IoT assets with mission critical applications
- Remote monitoring needs from NOC and unmanaged assets
- User identity and site/device based policy
- Ability to rapidly on-board sites into the network
- Eliminate any lateral propagation possibilities

VALIDATED ARCHITECTURE THAT PROVIDES

- User and device identity based policy
- Remote access via managed and unmanaged devices
- Micro-Segmentation of local LANs
- Templates for onboarding and policy changes
- Insane visibility for traffic monitoring

Energy & OT: Private 5G

CRITICAL NEEDS

- Isolation for critical OT environments
- Device and SIM-based identity
- High performance and reliability
- Policy-based access for internal/external resources
- Device type and activity monitoring

VALIDATED ARCHITECTURE THAT PROVIDES

- Private 5G with on-premise network functions
- Segmentation for mission critical traffic
- UE device identity-based policy
- Device fingerprinting and monitoring
- SLA for performance and reliability

RSAC 2025 Conference

Apply & Takeaways

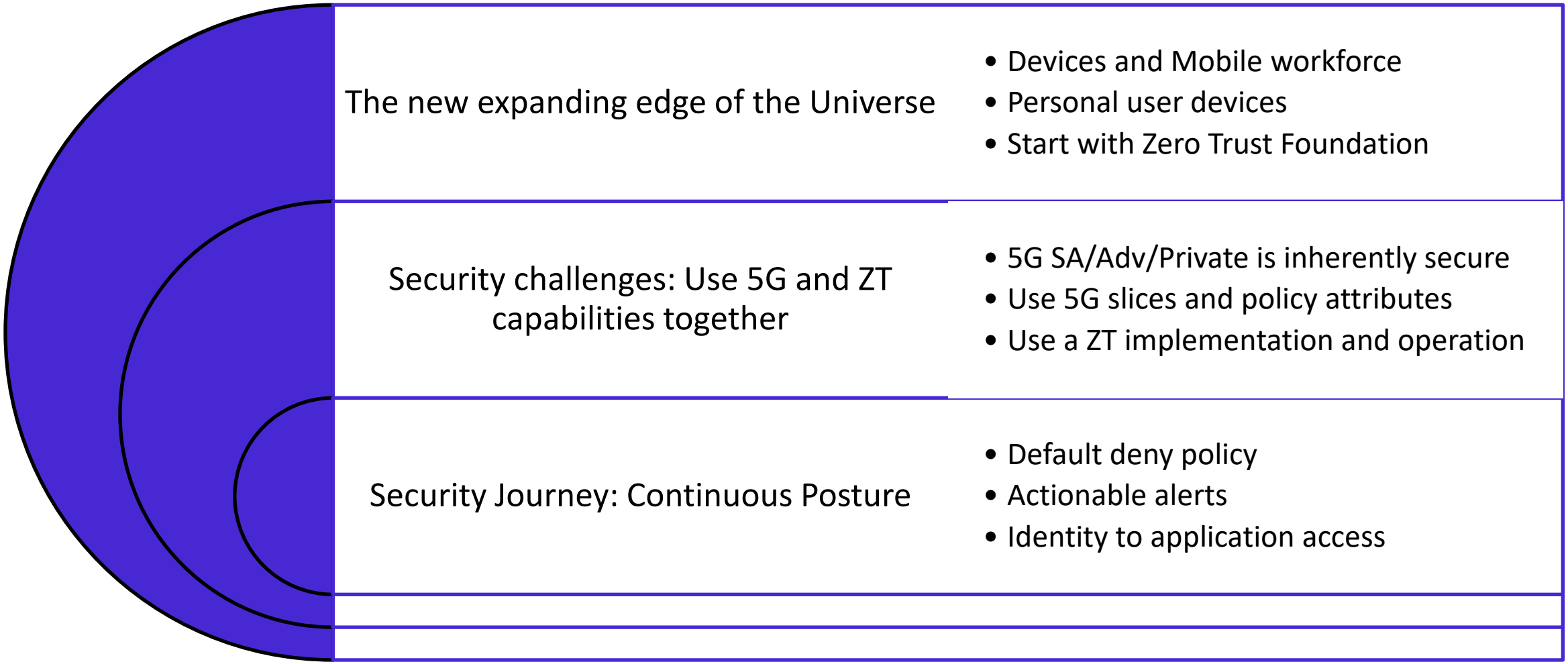
Apply: The Implementation Roadmap

Assess Attack Surface	• Know your networks, segments, users, devices, IoT, applications, mission critical needs – understand the attack surface and untrusted zones
Choose 5G Options / SASE	• Leverage slices, SIM Authentication, Policy enforcement with 5G attributes
Network Foundation	• Implement Secure Connectivity with User/Device/5G Identity based Policy and Segmentation
5G Edge to Cloud SDWAN	• Implement 5G SD-WAN for segmentation, encryption, resiliency, application specific performance
Private Resources Access	• Implement a Default Deny policy with Strict application layer-based rules to open access as needed
Internet Access	• Implement Hybrid Mesh Firewall, Browser Isolation, Data Leakage Prevention, and Malware/Phishing/Threat Detection to secure your assets & users
Unmanaged Devices	• Use Isolation based Secure Access Portals that protect your resources from untrusted users/devices

Apply: The Operational & Scaling Journey

The Policy Destination: 'Default Invisible'	Least Privilege Access : 'Identity>Application Access'	The Operational Objective: 'Actionable Alerts'
• A 'real' ZT implementation has granular policy implementation • Allow "Known Good", Deny "Known Bad" and Isolate/Monitor "Unknowns" • Monitor traffic patterns, and transition Unknowns to Knowns.	• Use User identity as well as Device / 5G (SIM and other attributes) identity • Allow access based on identity (and groups) and for specific Applications	• Tune Alerts from the system for visibility and action-ability • Develop a SOC alert operations system for actionable alerts.

Takeaways


The new expanding edge of the Universe
• Devices and Mobile workforce
• Personal user devices
• Start with Zero Trust Foundation
Security challenges: Use 5G and ZT capabilities together
• 5G SA/Adv/Private is inherently secure
• Use 5G slices and policy attributes
• Use a ZT implementation and operation
Security Journey: Continuous Posture
• Default deny policy
• Actionable alerts
• Identity to application access

RSAC 2025 Conference

Many Voices.
One Community.

Thank You!

Visit us: ericsson.com

Follow us (LinkedIn, X, Instagram): Ericsson Enterprise Wireless Solutions